ABSTRACT OF THE DISCLOSURE

Divided plaintexts, secret keys, public keys, random numbers, and the like are expressed in a polynomial representation, whereby a product-sum type cryptosystem is constituted on a finite field, whereby the cryptosystem is made resistive to attacks by LLL algorithm than a product-sum type cryptosystem on an integer ring. Divided plaintexts are encoded, and each term of the intermediate decrypted text is constituted of an error correcting code word, whereby the original plaintext is reproduced by the correction capability of the code word even when an error occurs.